

REMARKS**Status of the Claims**

Claims 1-51 are currently pending in the application. Of these, claims 1, 7, 13, 14, 22, 36 and 49-51 are independent. All claims have been rejected. No new matter is introduced by this amendment. Accordingly, entry of this Amendment is respectfully requested.

Rejections under 35 U.S.C. § 103

Claims 1-51 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over U.S. Patent No. 6,385,596 to Wiser et al. ("Wiser").

The rejection of claim 1 in the Office action reads as follows:

5. Regarding claim 1

Wiser discloses a method of processing information in a communications device, comprising: receiving from a first remote device content encrypted with a content key (e.g. col 4 ln 32-35); transmitting a request for the content key to a second remote device, the second remote device authorized to act on behalf of a provider of the content (e.g. col 4 ln 12-14); receiving from the second remote device an encrypted version of the content key, wherein the encrypted version of the content key is encrypted with a public key of the communications device (e.g. col 4 ln 34-36); and decrypting the encrypted version of the content key with a private key of the communications device, the private key of the communications device corresponding to the public key of the communications device. (e.g. col 4 ln 10-40).

6. Wiser does not specifically use the same order of steps as in the instant application. However, it would be obvious to one of ordinary skill in the art to merely re-order the steps in order to obtain the instant application and for greater convenience or economy.

The Wiser reference at (col. 3, line 67 to col. 4, line 12)., reads as follows:

"The purchase-quality audio data is encrypted when created by the artist with a media key,..." "This media key is then encrypted with a public key of the content manager." "The encrypted high-quality version of the song is combined with ... the media key into the media data file. The media data file is uploaded to the content manager for storage in the media data file system, where it can now be purchased by consumers. While in storage in the online music distribution system, the audio images remain encrypted and tied to the specific content manager."

The Wiser reference at (col. 4, lines 13-27)., reads as follows:

“To purchase a media data file, a consumer first registers with the media licensing center to obtain a digital passport. The passport is a combination of data that includes personal information uniquely identifying a user, ... and encryption key information used to encrypt media data for that person's use. The identifying information is typically the user's name, This information is combined in the passport with a public-private key pair generated by the media licensing center, into a digital certificate authenticating their identity.”

The Wiser reference at (col. 4, lines 32-41)., reads as follows:

“... First, the certificate is used to authenticate the purchaser to the content manager and delivery server.

Second, the purchaser's public key from the passport is used by the content manager to encrypt the media key for the media data file being purchased. In this manner, only the purchaser's media player can decrypt the media key for the purchased audio and playback the music. When the media player receives a media data file for playback, it uses the private key stored in the passport to decrypt the media key included in the media data file. The media key is then used to decrypt the audio image for playback at the user's machine.”

In response, the Applicant's Claim 1, Step (a) recites receiving the content from a first remote device, for example either the content distributor 104 or a first client device 108.

Applicant's Claim 1, Step (b) recites separately requesting the content key from a second remote device, the authorized agent 106 of the content distributor 104. Wiser only discloses requesting and receiving from the same device, Wiser's content manager 112, both the content and the content key. This is an important distinction because the Applicant has discovered how to redistribute the content from one client to another without sacrificing the encrypted security of the content, by using an authorized agent 106 of the content distributor 104 to handle the key encrypting keys. The Applicant's claimed invention is neither disclosed nor suggested in the Wiser reference.

This important distinction over the Wiser reference applies to all of the Applicant's independent claims 1, 7, 13, 14, 22, 36 and 49-51 and their respective dependent claims. The Wiser reference fails to disclose or suggest the Applicant's claimed invention of separately

requesting the content key from a different device than the device from which the content was obtained. The Applicant's claimed invention in claims 1-51 is neither disclosed nor suggested in the Wiser reference.

The Applicant's claimed invention overcomes a significant problem confronting the system disclosed in the Wiser reference, namely the network bottleneck created at Wiser's content manager 112 by satisfying the requests for the content from many clients 126. Wiser's content manager 112 stores the content encrypted under the media key and a copy of the media key encrypted under the content manager's public key. In Wiser, every client 126 that wants a copy of the content must request it from the content manager, which re-encrypts the media key under the public key of the requesting client 126 and then downloads it and the encrypted content to the requester.

By contrast, the Applicant's claimed invention enables any client 108 possessing an encrypted copy of the content, to redistribute that encrypted content to a second client 110, without needing to request a second download of the encrypted content from the Applicant's content distributor 104. The Applicant's claimed invention provides for an authorized agent 106 of the content distributor 104 and when the content encrypted under the content key is distributed, the content key is also distributed encrypted under the public key of the authorized agent 106. Thus, the claimed invention enables the encrypted security of the content to be maintained when it is received by a second client 110, because the content, which is encrypted under the content key, is distributed with the content key encrypted under the authorized agent's 106 public key. The second client 110 receives the content key encrypted under the authorized agent's 106 public key. The second client 110 then transmits a request for the content key to the

authorized agent 106 of the content distributor 104, and the agent re-encrypts the content key under the requester's 110 public key and returns it to the requester 110.

The Wiser reference fails to disclose or suggest the Applicant's claimed invention of separately requesting the content key from a different device than the device from which the content was obtained.

Accordingly, Applicant respectfully requests that this rejection be withdrawn.

CONCLUSION

Based on the foregoing amendments and remarks, Applicants respectfully request reconsideration and withdrawal of the rejection of claims and allowance of this application.

AUTHORIZATION

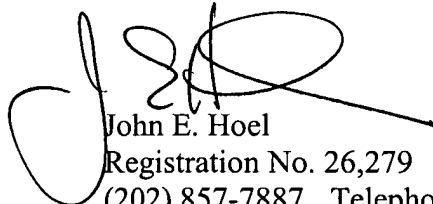
The Commissioner is hereby authorized to charge any additional fees which may be required for consideration of this Amendment to Deposit Account No. 13-4500, Order No. 4208-4143. A DUPLICATE OF THIS DOCUMENT IS ATTACHED.

In the event that an extension of time is required, or which may be required in addition to that requested in a petition for an extension of time, the Commissioner is requested to grant a petition for that extension of time which is required to make this response timely and is hereby authorized to charge any fee for such an extension of time or credit any overpayment for an extension of time to Deposit Account No. 13-4500, Order No. 4208-4143. A DUPLICATE OF THIS DOCUMENT IS ATTACHED.

Respectfully submitted,
MORGAN & FINNEGAN, L.L.P.

Dated: April 5, 2006

By:


John E. Hoel
Registration No. 26,279
(202) 857-7887 Telephone
(202) 857-7929 Facsimile

Correspondence Address:

MORGAN & FINNEGAN, L.L.P.
3 World Financial Center
New York, NY 10281-2101